Office of Inspector General

Status Report of Laptops Investigation

November 21, 2006

This is the third in a series of status reports on the investigation of the loss of Sensitive Personally Identifiable Information (SPII) on two Office of Inspector General (OIG) laptop computers.

In July 2006, a thief stole an OIG Special Agent's laptop computer from a locked government vehicle in Doral, Florida, near Miami. This laptop contained SPII (an individual's name plus other identifying information such as Social Security number or date of birth) for thousands of Florida residents. This theft and the discovery that SPII was involved led the then-Acting Inspector General to order an investigation not only of the Miami-area theft, but also of an earlier theft of an OIG laptop that occurred in Orlando, Florida, in April 2006.

In response to the thefts, we launched efforts to recover the laptops, review backup disks to determine the laptops' contents, notify the individuals whose information was on the laptops, and determine if our policies were followed and whether they need to be strengthened. Our continuing investigation has shown with a high degree of confidence that the two laptops were not stolen to exploit the data for identity theft. There has been no credit fraud resulting from the theft of either laptop and based on our investigation to date, we believe that the risk of credit fraud in the future is very low. The investigation is nearly complete and we expect to issue a report by the end of the year. Today, however, we would like to report two notable developments that have occurred.

Two Arrested After Theft of Decoy Laptop Computer

First, surveillance and investigation by our Special Agents, with assistance from the Federal Bureau of Investigation and the Miami-Dade County Police Department, led to the arrest of an individual suspected of having stolen the Miami-area laptop. This suspect was identified in a surveillance operation

conducted at the same restaurant where this laptop had been stolen. During our surveillance, this individual stole a decoy computer—using the same technique that was used in the original theft (a device was used to "punch" the lock in the passenger-side door).

The suspect admitted stealing numerous laptops but did not admit to stealing the Special Agent's laptop on July 27. Considering the time that passed before his arrest, however, it is questionable whether the suspect could have known whether one of the laptops he admitted stealing was or was not the laptop stolen on July 27. This individual was indicted on a Federal charge of theft of government property (the decoy laptop).

The decoy laptop stolen during our surveillance was delivered to a computer business owner, who loaded new operating system software on it. Loading new operating system software overwrites some of the data on the hard disk and makes any remaining data invisible to the new owner and very difficult to recover without specialized knowledge and tools.

After we recovered the decoy computer, we performed a forensic analysis confirming that the original data on the computer had not been accessed before the new operating system was loaded. Interviews of these subjects and other involved individuals revealed the existence of a small theft ring that stole laptops at and near the restaurant, loaded new operating systems, and then sold the computers on the used computer market—primarily to high school students. The interviews also confirmed that the ring did not target the data and did not even attempt to access the data on the laptops they stole.

An investigation of the Orlando theft is continuing.

Data Breach Analysis Shows No Misuse of Data

The second development is that we contracted with an Identity Risk Management company to review SPII data for almost 133,000 individuals on the Miami-area laptop and almost 9,500 individuals on the Orlando laptop (those same 9,500 individuals were also on the Miami-area laptop). The review found no indication that the data had been misused as of November 13, 2006. OIG will continue to receive periodic reports on whether there is an indication of suspicious activity that involves organized misuse of SPII from the laptops.

We awarded a contract to ID Analytics, Inc., of San Diego, California, to provide data breach analysis services to determine whether SPII for the approximately 133,000 pilots, commercial truck drivers, and individual drivers' license holders in Florida was being exploited. This firm has developed proprietary software to

monitor identity activity to determine whether identity theft is occurring in an organized way (indicating that stolen data is being exploited) and identifying how the data is being exploited (assisting investigators in apprehending the criminals). It has access to real-time identity fraud information, including data from leading companies that gather information from applications for credit, change of address, and other identity risk information. The companies include six of the top 10 U.S. banks, almost all major wireless carriers, and leading retail credit card issuers.

Data breach analysis is recommended by the President's Task Force on Identity Theft (Task Force) as a useful tool to track the incidence of credit fraud and identity theft and determine whether it is the result of a loss of SPII. In its September 19, 2006, memorandum, the Task Force said: "Such technology may be useful for incidents involving data for large numbers of individuals."

The Task Force also said, "for any large breach, it is statistically predictable that a certain number of the potential victim class will be victims of identity theft through events other than the data security breach in question. Data-breach monitoring of the type described here can assist an agency in determining whether the particular incident it has suffered is truly a source of identity theft, or whether, instead, any such reports are the normal by-product of the routine incidence of identity theft." The memo is available at:

http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf

OIG Hotline Still in Operation

As of November 13, 2006, our Hotline has received over 1,600 phone calls, emails, and letters, and responded with information and instructions on how to request that the major credit reporting bureaus place a fraud alert on their accounts. We have provided a telephone or email response to every individual who requested one. Of the communications that OIG received, nearly 50 produced possible leads in the criminal investigation. The Hotline remains in operation 24 hours a day, 7 days a week, at (800) 424-9071 and by email at hotline@oig.dot.gov. The Hotline's Data Security Portal, with previous status reports and other information and advice related to the laptops, is available on our website as well. The address is *www.oig.dot.gov/datasecurity.jsp*.